(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 199 46 959 A 1**

(51) Int. Cl.[7]: G 06 F 9/445

(21) Aktenzeichen: 199 46 959.8
(22) Anmeldetag: 30. 9. 1999
(43) Offenlegungstag: 12. 4. 2001

DE 199 46 959 A 1

(71) Anmelder:
Siemens PC Systeme GmbH & Co KG, 86199 Augsburg, DE

(74) Vertreter:
Epping, Hermann & Fischer GbR, 80339 München

(72) Erfinder:
Munker, Thomas, 86633 Neuburg, DE; Mayer, Friedrich, 86153 Augsburg, DE; Rzedkowski, Ryszard, 86152 Augsburg, DE; Altmann, Helmut, 82110 Germering, DE; Michel, Uwe, 86343 Königsbrunn, DE

(56) Entgegenhaltungen:

US	59 30 504 A
EP	08 03 812 A1
WO	97 13 202 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zum Laden von Daten für grundlegende Systemroutinen

(57) Die Erfindung betrifft ein Verfahren zum Laden von Daten für grundlegende Systemroutinen (BIOS) eines Datenverarbeitungssystems in einem nichtflüchtigen Speicher. Hierfür wird zunächst eine vom Betriebssystem unabhängige Schnittstelle in den grundlegenden Systemroutinen bereitgestellt. Der Prozessor des Datenverarbeitungssystems wird in einem System-Mangement-Modus über diese Schnittstelle versetzt, und darauf erfolgt das Einschreiben neuer Daten für grundlegende Systemroutinen in den nichtflüchtigen Speicher. Vorzugsweise ist der System-Management-Modus ein ununterbrechbarer Interrupt mit Task-Switch und somit für das Betriebssystem transparent.

DE 199 46 959 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren zum Laden von Daten für grundlegende Systemroutinen und insbesondere ein Verfahren für eine Auffrischung (Update) von Daten für grundlegende Systemroutinen über eine vom Betriebssystem unabhängige Schnittstelle.

Datenverarbeitungssysteme, wie beispielsweise Personal Computer oder Controller für Geräte oder Maschinen, werden üblicherweise erst nach dem Laden von grundlegenden Systemroutinen beispielsweise BIOS(Basic-Input-Output-System-Daten) in den Arbeitsspeicher der zentralen Verarbeitungseinheit (CPU) voll funktionsfähig. Auch ohne Betriebssystem benötigen die Datenverarbeitungssysteme eine Grundfunktionalität, mit der elementare Operationen ausgeführt werden können. Solche elementaren Operationen sind beispielsweise Routinen für die Eingabe von Zeichen über die Tastatur sowie deren Ausgabe auf den Bildschirm und den Drucker, eine Routine für das Laden des Betriebssystems in den Arbeitsspeicher, sowie Prüfroutinen für einen automatisch ablaufenden Selbsttest beim Anschalten des Datenverarbeitungssystems. Diese Operationen werden auch als grundlegende Systemroutinen (BIOS) bezeichnet. Das BIOS enthält darüber hinaus auch Spezifikationen bezüglich der einzelnen Hardwarekomponenten, beispielsweise der mit dem Computer verbundenen Laufwerke, externen Schnittstellen, Graphikkarten usw.

Die zum Ausführen dieser Systemroutinen erforderlichen Daten werden in einem nichtflüchtigen Speicherbaustein der Datenverarbeitungsanlage, beispielsweise einem PROM (Programmable Read Only Memory), einem EPROM (Electrical Programmable Read Only Memory), einem FLASH usw. dauerhaft gespeichert.

Da die grundlegenden Systemroutinen die Arbeitsweise eines Datenverarbeitungssystems wesentlich beeinflussen, ist es gelegentlich erforderlich, eine überarbeitete Version der grundlegenden Systemroutinen in der Datenverarbeitungsanlage einzusetzen, also das BIOS updaten. Dies kann durch einen Austausch des Speicherbausteins erfolgen, was allerdings den Nachteil hat, daß dies nur durch entsprechend qualifiziertes Personal und vor Ort erfolgen kann.

Ist anstelle eines nichtüberschreibbaren PROM-Bausteins ein überschreibbarer Speicherbaustein, beispielsweise ein EPROM- oder ein FLASH-Baustein in dem Datenverarbeitungssystem vorhanden, dann können die grundlegenden Systemroutinen in diesem Speicherbaustein überschrieben werden. Dies hat den Vorteil, daß kein geschultes Personal und kein Eingriff in die Hardware des Systems erforderlich ist. Ein Beispiel hierfür ist das von der Fa. ACER benutzte Verfahren. Bei dem ACER Verfahren sind das FLASH-Programm und Daten zum Updaten auf einer Festplatte (HD) gespeichert. Beim Booten wird ein spezielles Mini-Betriebssystem geladen, und die hardwarenahe Anwendersoftware führt den BIOS-Update durch. Danach wird zunächst ein Reboot durchgeführt, und dann wird erst das eigentliche Betriebssystem für den Anwender geladen.

Ein anderes Beispiel ist das Desk-Flash-Verfahren, das in der DE-C 197 52 615 offenbart. Dieses Verfahren bietet gegenüber dem ACER-Verfahren den Vorteil, daß die Möglichkeit besteht, den BIOS-Update im laufenden Betrieb des Datenverarbeitungssystems ohne weitere Beeinträchtigungen des Systems durchzuführen. Dies bietet unter anderem die Möglichkeit, in einem Computernetzwerk über einen Administrator-PC einen BIOS-Update ohne Reboot der mit dem Computernetzwerk verbundenen einzelnen PCs "remote", also räumlich getrennt, durchzuführen.

Ein Nachteil des vorstehend beschriebenen bekannten Verfahrens ist, daß diese hardwarenahen und deshalb hardwareabhängige Verfahren auf beliebigen PC-Systemen lauffähig sein müssen und deshalb immer wieder an neue Hardwarekonfigurationen angepaßt werden müssen. Diese Anpassung muß für jedes zu unterstützende Betriebssystem erfolgen. Das heißt, die Anzahl der nötigen Anpassungen ergibt sich aus der Zahl der unterschiedlichen PC-Systemboards multipliziert mit der Zahl der zu unterstützenden Betriebssysteme. Weitere Nachteile bestehen darin, daß ein Debugging leicht durchzuführen ist, und daß das System offen für Fremdzugriffe und damit auch für Viren ist.

Eine Aufgabe der Erfindung ist es daher, ein Verfahren zu schaffen, das eine verringerte Anzahl von Anpassungen beim Update der grundlegenden Systemroutinen ermöglicht, wobei eine Auffrischung bei laufendem Betriebssystem möglich sein soll.

Erfindungsgemäß wird die Aufgabe durch ein Verfahren nach Anspruch 1 gelöst. Die abhängigen Ansprüche betreffen weitere vorteilhafte Aspekte der Erfindung.

Das erfindungsgemäße Verfahren zum Laden von Daten für grundlegende Systemroutinen eines Datenverarbeitungssystems in einen nichtflüchtigen Speicher gekennzeichnet durch die Schritte: Bereitstellen einer vom Betriebssystem unabhängigen Schnittstelle in den grundlegenden Systemroutinen, Auslesen von neuen Daten aus einem externen Speichermedium, Versetzen eines Prozessors des Datenverarbeitungssystems in einen System-Management-Modus über diese Schnittstelle, und Einschreiben der neuen Daten für grundlegende Systemroutinen sowie gegebenenfalls die Daten des Micro Code Update in den nichtflüchtigen Speicher durch Aufsetzen eines FLASH-Programmes.

Durch das erfindungsgemäße Verfahren wird die Anzahl der Anpassungen deutlich verringert, da sich die Anzahl der nötigen Anpassungen nun aus der Zahl der unterschiedlichen PC-System-Boards zuzüglich einmalig der Zahl der zu unterstützenden Betriebssysteme ergibt. Ein weiterer Vorteil besteht darin, daß keine Dateisystemabhängigkeit besteht.

Entsprechend einem weiteren vorteilhaften Aspekt der Erfindung ist der System-Management-Modus ein ununterbrechbarer Interrupt mit Task-Switch. Das heißt, dieser Modus ist für das Betriebssystem vollkommen transparent.

Vorzugsweise wird nach dem Einschreiben neuer Daten das Datenverarbeitungssystem zum Aktivieren neu gestartet, so daß das System mit den Daten der neuen grundlegenden Systemroutinen arbeiten kann.

Ein weiterer Vorteil der Erfindung ergibt sich daraus, daß das Laden der Daten für neue grundlegende Systemroutinen über einen räumlich getrennten Administrator-Computer in einem Computernetzwerk ohne Reboot erfolgen kann. Insbesondere bei Computernetzwerken erleichtert dies die Arbeit beim Updaten des BIOS der einzelnen PCs.

Wesentliche Vorteile der Erfindung sind, daß eine Anpassung der hardwarenahen Anwendersoftware an die verschiedenen Hardwarekonfigurationen nicht mehr erforderlich ist. Dieser erfolgt bereits mit der Bereitstellung und Freigabe der Fertigungs-BIOS. In vorteilhafter Weise ist auch weniger Testaufwand erforderlich und der Prozess kann schneller ablaufen. Das Datenverarbeitungssystem beinhaltet die hardwarenahen Teile der Anwendersoftware. Gegenüber dem bekannten Verfahren von ACER erfolgt das Auffrischen des BIOS bei laufendem Betriebssystem, sodaß es ohne Störung des PC-Anwenders erfolg n kann.

Das Bereitstellen und Ausnutzen ein r vom Betriebssystem unabhängigen Schnittstelle hat folgende Vorteile. Der System-Management-Modus kann derart ausgestaltet sein, daß er nur über ein spezielles SMI-Signal (System-Management-Interrupt-Signal) erreichbar ist, so daß er nur über den RSM-Befehl (Reset-System-Management-Befehl) beendet werden kann. Dieser RSM-Befehl kann derart ausgestaltet

sein, daß er nur im System-Management-Modus ausgeführt wird und ansonsten als unzulässiger Betriebscode behandelt wird.

Der System-Management-Modus kann nicht durch äußere Ereignisse (Interrupts, NMI, usw.) unterbrochen oder beeinflußt werden. Außerdem liegt der spezifische Code für den System-Management-Modus in dem Speicherbereich des nichtflüchtigen Speichers (SMRAM), welcher mittels Hardware vor dem Betriebssystem geschützt und vor ihm abgeschottet ist. Dies sichert den ausführungsspezifischen Codeteil für den System-Management-Modus und die zugehörigen Daten vor Fremdzugriff und damit auch gegen Viren.

Eine vorteilhafte Ausgestaltung des erfindungsgemäßen Verfahrens ist dadurch gekennzeichnet, daß im System-Management-Modus ein ununterbrechbarer Interrupt mit Task-Switch genutzt wird, wobei dieser Modus für das Betriebssystem transparent wird.

Eine weitere vorteilhafte Ausgestaltung des erfindungsgemäßen Verfahrens ist dadurch gekennzeichnet, daß die neuen Daten für die grundlegenden Systemroutinen fragmentiert und in einem RAM abgelegt werden können, wodurch der Prozess flexibler gestaltet wird, wenn es um die Berücksichtigung spezieller Erfordernisse der Soft- beziehungsweise Hardware geht. Außerdem werden gegenüber dem Verfahren von ACER damit die Anzahl der Fehlerquellen reduziert.

Eine weitere vorteilhafte ausgestaltung des erfindungsgemäßen Verfahrens ist dadurch gekennzeichnet, daß, wenn der Prozessor sich im System-Management-Modus befindet, die Daten darauf überprüft werden, ob die Daten vollständig sind und ob die Daten die zu den grundlegenden Systemroutinen passenden Daten sind. Damit werden Fehler bei der Durchführung des Verfahrens vermieden.

Eine weitere vorteilhafte Ausgestaltung des erfindungsgemäßen Verfahrens ist dadurch gekennzeichnet, daß nach dem Einschreiben neuer Daten in dem nichtflüchtigen Speicher das Datenverarbeitungssystem zum Aktivieren nur einmal neu gestartet werden muß, sodaß das System nun mit den Daten der neuen grundlegenden Systemroutinen arbeiten kann.

Eine weitere vorteilhafte Ausgestaltung des erfindungsgemäßen Verfahrens ist dadurch gekennzeichnet, daß das Laden der Daten für neue grundlegende Systemroutinen über einen räumlich getrennten Administrator-Computer in einem Computernetzwerk ohne Reboot erfolgen kann. Insbesondere bei Computernetzwerken erleichtert dies die Arbeit beim Updaten des BIOS der einzelnen PCs.

Schließlich ist eine weitere vorteilhafte Ausgestaltung des erfindungsgemäßen Verfahrens dadurch gekennzeichnet, daß bei einem Multiprozessorsystem alle Prozessoren synchronisiert beziehungsweise in den System-Management-Modus versetzt werden, und daß zum Betriebssystem zurückgekehrt wird, wenn der FLASH- beziehungsweise Teilflash-Vorgang beendet ist. So kann bei Multiprozessorsystemen die erforderliche exklusive Nutzung der Systeme und Ressourcen sowie insbesondere der Zugriff auf den nichtflüchtigen Speicher im System-Management-Modus(SMM) gelöst werden.

Im folgenden wird die Erfindung detailliert anhand eines Ausführungsbeispiels beschrieben.

In einem Datenverarbeitungssystem ist auf einer Systemplatine ein nichtflüchtiger Speicher, nachfolgend als FLASH bezeichnet, angeordnet. Beim FLASH kann es sich um einen Speicherbaustein handeln, dessen Speicher in Sektoren einer Größe von beispielsweise 64 kB eingeteilt sind. Innerhalb der Sektoren können einzelne Bytes adressiert und beschrieben werden. Ein Löschvorgang wird üblicherweise durchgeführt, indem immer ein gesamter Sektor gelöscht wird. Das Datenverarbeitungssystem kann mit Hilfe des im FLASH gespeicherten BIOS ein B triebssystem in einen Arbeitsspeicher (nicht dargestellt) einer CPU laden, wodurch es in einem betriebsfähigen Zustand versetzt wird. Wünschenswert ist es nun, daß ein Auffrischen des BIOS unabhängig von dem jeweiligen Betriebssystem des Datenverarbeitungssystems und der jeweiligen Hardware (aus Software-Sicht) ohne Anpassung der einmal erstellten Software auf neue Hardware möglich ist.

Erfindungsgemäß wird hierfür eine Standardschnittstelle in dem BIOS geschaffen, nämlich die sogenannte BIOS-Service-API-Schnittstelle (API = Application Programming Interface). Diese Schnittstelle ist ein Programm, das unabhängig von Betriebssystem den Lese- und Schreibvorgang für grundlegende Systemroutinen in den nichtflüchtigen Speicher steuert. Auf diese Art wird eine Trennung der hardwarenahen Daten und der betriebssystemnahen Daten erreicht, so daß die Anzahl der Anpassungen nicht mehr das Produkt der Anzahl der unterstützten Betriebssysteme mit der Anzahl der Systemboards ist, sondern nur noch die Summe dieser beiden Größen.

Ein FLASH-Programm lädt neue Daten für grundlegende Systemroutinen aus einem externen Speicher in das RAM des Datenverarbeitungssystems. Diese Daten können auch fragmentiert sein.

Das Datenverarbeitungssystem wird vom FLASH-Programm über die oben genannte BIOS-Service-API mittels eines SMI-Signals in einen "System-Management-Modus" versetzt.

Wenn das System dann in dem System-Management-Modus arbeitet, ist es vom jeweiligen Betriebssystem unabhängig. Aus Sicht des Betriebssystems ist der System-Management-Modus ein ununterbrechbarer Interrupt mit Task-Switch, d. h. vollkommen transparent. Dies hat den Vorteil, daß unabhängig von dem jeweiligen Betriebssystem des Datenverarbeitungssystems das neue BIOS geladen werden kann.

Da das BIOS-Service-API standardisiert ist, ist es ausreichend, im Rahmen der BIOS-Entwicklung für das jeweilige PC-Systemboard und einmalig das FLASH-Programm für die zu unterstützenden Betriebssysteme zu erstellen. Diese beiden Anpassungen sind unabhängig voneinander.

Während das System in dem System-Management-Modus ist, ist es unabhängig von äußeren Einflüssen, wie beispielsweise Interrupts und ähnlichem. Nur durch einen besonderen Befehl oder ein Ausschalten des Datenverarbeitungssystems kann das Updaten des BIOS unterbrochen werden, woraus sich eine erhöhte Sicherheit ergibt.

Um eine Fehlfunktion aufgrund fehlerhafter Manipulation an dem BIOS zu vermeiden, ist der System-Management-Modus-Code vorzugsweise in einem getrennten Speicherbereich des nicht-flüchtigen Speichers (SMRAM), welcher durch Hardwaremaßnahmen vor dem Betriebssystem geschützt ist, und diesem abgeschottet ist. Es heißt, dieser Teil des BIOS, der für Laden und Archivieren verantwortlich ist, ist gegenüber dem Betriebssystem abgeschottet und geschützt. Auf diese Art sind die für die Ausführung relevanten Codeteile sowie die zugehörigen Daten vor Fremdzugriff geschützt.

Darüber hinaus bietet sich bei Multiprozessor-Systemen die Möglichkeit, die erforderliche exklusive Nutzung der Systemressourcen mit Hilfe der BIOS-Service-API zu lösen. Dabei werden alle anderen Prozessoren ebenfalls in den System-Management-Modus gesetzt, und es wird erst wieder zum Betriebssystem zurückgekehrt, wenn der FLASH-Vorgang gültig beendet ist.

Gegenüber dem bekannten Desk-Flash-Programm wird

eine standardisierte Schnittstelle zur Anpassung an unterschiedliche Hardwarekonfigurationen bereitgestellt, wobei die Anpassung der für das Betriebssystem spezifischen Anwendungen nicht mehr erforderlich ist.

Obwohl die Erfindung anhand eines bestimmten Ausführungsbeispiels beschrieben wurde, ist sie auf dieses nicht beschränkt. Verschiedene Abwandlungen und Modifikationen sind für den Fachmann ersichtlich. Beispielsweise können je noch dem Betriebssystem OS oder Software-Architektur verschiedene, auch mehrere, Software-Layer aufgelegt werden.

Auch ist die Erfindung nicht auf ein Datenverarbeitungssystem, beispielsweise mit BIOS, beschränkt, sondern bezieht sich generell auf Controller, die ein Betriebssytem beziehungsweise Firmware aufweisen, für Geräte und Maschinen, beispielsweise Mobiltelefongeräte, controllergesteuerte Hausgeräte oder NC-Maschinen.

Patentansprüche

1. Verfahren zum Laden von Daten für grundlegende Systemroutinen eines Datenverarbeitungssystems in einem nicht-flüchtigen Speicher **gekennzeichnet durch** die Schritte:
   - Bereitstellen einer betriebssystemunabhängigen Schnittstelle in den grundlegenden Systemroutinen,
   - Auslesen der neuen Daten aus einem externen Speichermedium, und Schreiben in RAM
   - Versetzen eines Prozessors des Datenverarbeitungssystems in einen System-Management-Modus über diese Schnittstelle, und
   - Einschreiben neuer Daten für grundlegende Systemroutinen sowie gegebenenfalls die Daten des Micro Code Update in den nichtflüchtigen Speicher.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass im System-Management-Modus ein ununterbrechbarer Interrupt mit Task-Switch genutzt wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die neuen Daten für die grundlegenden Systemroutinen fragmentiert und in einem RAM abgelegt werden

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass wenn der Prozessor sich im System-Management-Modus befindet, die Daten darauf überprüft werden, ob die Daten vollständig sind und ob die Daten die zu den grundlegenden Systemroutinen passenden Daten sind.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass nach dem Einschreiben neuer Daten in dem nichtflüchtigen Speicher das Datenverarbeitungssystem zum Aktivieren der Daten neu gestartet wird.

6. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass bei dem das Laden der Daten für neue grundlegende Systemroutinen über einen räumlich getrennten Administrator-Computer eines Computernetzwerks verfolgt.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass bei einem Multiprozessorensystem alle Prozessoren synchronisiert beziehungsweise in den System-Management-Modus versetzt werden, und dass zum Betriebssystem zurückgekehrt wird, wenn der FLASH-Vorgang beendet ist.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass neue Daten für die grundlegenden Systemroutinen nur teilweise in den nichtflüchtigen Speicher eingeschrieben werden.

9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Daten des nichtflüchtigen Speichers ausgelesen, auch teilweise, und auf einem externen Speichermedium geschrieben werden.